



<b>Return</b>		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
<b>Certification</b>		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between; align-items: flex-end;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 65%;"> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Executing officer's signature</i></p> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Printed name and title</i></p> </div> </div>		

## **ATTACHMENT A**

### **Property to Be Searched**

1. The property to be searched are seven (7) electronic storage devices currently held at the Bureau of Alcohol, Tobacco, Firearms and Explosives, 1000 N. Water Street, Suite 1400, Milwaukee, Wisconsin, which can be further described as:

- a. Samsung Smartphone (model unknown, IMEI: 352612262310911, ATF item no. 0046, **TARGET DEVICE 1**);
- b. Purple Apple iPhone (model unknown, serial no. unknown, ATF item no. 0052, **TARGET DEVICE 2**);
- c. Motorola smartphone with light blue case, ATF item no. 0053 , **TARGET DEVICE 3**);
- d. Black Amazon tablet (model unknown, ATF item no. 0047, **TARGET DEVICE 4**);
- e. Black Dell Desktop Computer (model unknown, ATF item no. 0054, **TARGET DEVICE 5**);
- f. Black Lenovo laptop computer (model unknown, ATF item no. 0051, **TARGET DEVICE 6**); and,
- g. External hard drive (make/model unknown, ATF item no. 49, **TARGET DEVICE 7**).

## **ATTACHMENT B**

### **Particular Things to be Seized**

1. All records on the seven electronic devices related to violations of 18 U.S.C. §§ 1956 and 1957 (conspiracy to commit money laundering and money laundering), and 21 U.S.C. §§ 846 and 841 (conspiracy to distribute, possession with intent to distribute and distribution of controlled substances) including:
  - a. lists of contacts with any identifying information;
  - b. photographs, videos, or other media storage connected to the enumerated violations;
  - c. types, amounts, and prices of drugs purchased/sold;
  - d. any information related to sources or purchasers of drugs (including names, addresses, phone numbers, or any other identifying information);
  - e. all bank records, checks, credit card bills, account information, and other financial records related to the enumerated violations.
2. Any and all financial records connected to the purchase/sale of drugs and money laundering;
3. Documentation establishing the identity of the individuals in control of the residences;
4. Any and all financial records connected to the purchase/sale of drugs and money laundering, and any correspondence regarding other drug sellers and/or purchasers;
5. Any evidence of illegal drugs or controlled substances;
6. Any evidence of proceeds of drug trafficking activities, including United States currency;

7. All bank records, checks, credit card bills, account information, and other financial records; financial records, documents, statements, or other evidence of control of bank or other financial accounts and investment funds;

8. List of drug customers and related identifying information;

9. Personal address books, telephone bills, photographs, letters, personal notes, documents and other items or lists reflecting names, addresses, telephone numbers, addresses and communications regarding illegal activities among and between members and associates involved in drug trafficking activities;

10. Any evidence of documents and deeds reflecting the purchase or lease of items obtained with the proceeds from drug trafficking activities;

11. Records of off-site locations to store proceeds and other records, including safes, vaults, or lock boxes, safe deposit box keys, records and receipts and rental agreements for storage facilities;

12. Records of mail and communications services, cellular telephones and all electronic storage areas on the devices including stored telephone numbers, recently called numbers list, text messages, digital audio and or video recordings, pictures, settings, and any other user defined settings and/or data;

13. Evidence of indicia of occupancy, residency or ownership of premises, including utility bills, telephone bills, loan payment receipts, addressed envelopes, escrow documents and keys;

14. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

15. Records evidencing the use of the Internet Protocol address, including:
  - a. records of Internet Protocol addresses used;
  - b. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

## UNITED STATES DISTRICT COURT

for the  
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)

Seven electronic devices currently located at 1000 N. Water Street,  
Suite 1400, Milwaukee, WI, more fully described in Attachment A.

Case No.23-911 M(NJ)

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the \_\_\_\_\_ Eastern \_\_\_\_\_ District of \_\_\_\_\_ Wisconsin \_\_\_\_\_, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☐ contraband, fruits of crime, or other items illegally possessed;  
☐ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:


Code Section	Offense Description
18 U.S.C. §§ 1956 and 1957	Conspiracy to commit money laundering and money laundering
18 U.S.C. §§ 846 and 841	Conspiracy to distribute controlled substances and possession with intent to distribute and distribution of controlled substances

The application is based on these facts:

See Attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

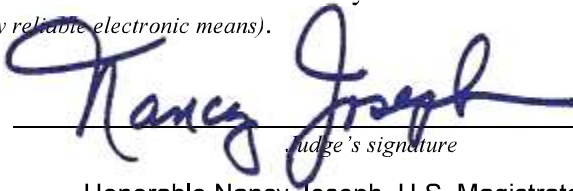
  
Applicant's signature

Sean Carlson, Special Agent, ATF

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
\_\_\_\_\_ telephone \_\_\_\_\_ (specify reliable electronic means).

Date: 4/25/2023

  
Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT

I, Sean Carlson, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property, three cellphones, one tablet computer, one desktop computer, one laptop computer, and one external hard drive and the extraction of evidence described in Attachment B.

2. I am employed as a Special Agent with the United States Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives (“ATF”) assigned to the Milwaukee Field Office since November 2015. I have been employed as a full-time law enforcement officer for approximately fifteen years. Prior to my employment at ATF, I was a Patrol Officer at the Hammond Police Department in Hammond, Indiana for over four (4) years, and then I served approximately five (5) years as a Federal Air Marshal with the U.S. Department of Homeland Security.

3. As a Special Agent, I have participated in the investigation of firearms and narcotics-related offenses with a money laundering component, resulting in the prosecution and conviction of numerous individuals and the seizure of illegal drugs, and weapons. As a firearms investigator, I have interviewed many individuals involved in firearm and drug trafficking and have obtained information from them regarding acquisition, sale, importation, manufacture, and distribution of firearms and controlled substances. Through my training and experience, I am familiar with the actions, habits, traits, methods, and terminology utilized by the traffickers and abusers of controlled substances.



4. Based on my training, experience and participation in drug trafficking, to include money laundering and firearms trafficking investigations, I know and have observed the following:

5. I have relied on informants to investigate firearms trafficking and drug trafficking. Through informant interviews and debriefings of individuals involved in those offenses, I have learned about the manner in which individuals and organizations finance, purchase, transport, and distribute firearms and narcotics both within and outside of Wisconsin. I have utilized informants to conduct “controlled purchases” of firearms and controlled substances from individuals, as opposed to licensed gun dealers. I have also conducted surveillance of individuals engaged in firearms, drug trafficking, and money laundering and participated in the execution of numerous search warrants resulting in the seizure of drugs, financial information related to narcotics trafficking, firearms, ammunition, and magazines.

6. Based on my training and experience, I have become familiar with the language utilized over the telephone to discuss firearms and drug trafficking, to include money laundering, and know that the language is often limited, guarded, and coded. I also know that firearms and drug traffickers often use electronic devices (such as computers and cellular phones) and social media to facilitate these crimes. Based on my experience, I know that narcotics and firearms traffickers may keep photographs of these items on electronic devices.

7. I also know that drug traffickers and firearms traffickers commonly possess—on their person, at their residences, at their places of business, in their vehicles, and other locations where they exercise dominion and control items related to drug trafficking and money laundering.

8. I know that those engaged in unlawful conduct such as narcotics trafficking often put their telephones in nominee names to distance themselves from telephones that are utilized to facilitate these and related offenses. I also know that drug traffickers often use proceeds to purchase assets such as vehicles, property, jewelry, and narcotics. I also know that drug traffickers often use nominees to purchase or title these assets to avoid scrutiny from law enforcement.

9. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other investigators and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

10. There is probable cause to believe that evidence of violations of the following laws of the United States, including the things described in Attachment B, will be found in the property listed in Attachments A, respectively: 21 U.S.C. Sections 846 and 841 (conspiracy to distribute controlled substances and possession with intent to distribute and distribution of controlled substances); and Title 18, U.S.C. Sections 1956 and 1957 (conspiracy to commit money laundering and money laundering) is housed within the below mentioned electronic devices.

11. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other investigators and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

### **IDENTIFICATION OF PROPERTY TO BE SEARCHED**

12. The property to be searched are seven (7) electronic storage devices currently held at the Bureau of Alcohol, Tobacco, Firearms and Explosives, 1000 N. Water Street, Suite 1400, Milwaukee, Wisconsin, which can be further described as:

- a. Samsung Smarthphone (model unknown, IMEI: 352612262310911, ATF item no. 0046, **TARGET DEVICE 1**);
- b. Purple Apple iPhone (model unknown, serial no. unknown, ATF item no. 0052, **TARGET DEVICE 2**);
- c. Motorola smartphone with light blue case, ATF item no. 0053 , **TARGET DEVICE 3**);
- d. Black Amazon tablet (model unknown, ATF item no. 0047, **TARGET DEVICE 4**);
- e. Black Dell Desktop Computer (model unknown, ATF item no. 0054, **TARGET DEVICE 5**);
- f. Black Lenovo laptop computer (model unknown, ATF item no. 0051, **TARGET DEVICE 6**); and
- g. External hard drive (make/model unknown, ATF item no. 49, **TARGET DEVICE 7**).

The applied-for warrant would authorize the search and recovery of evidence particularly described in Attachment B.

### **PROBABLE CAUSE**

13. In January 2019, United States Postal Service Office of the Inspector General (USPS OIG) Special Agent (SA) Edward O'Dwyer and Milwaukee Police Department Detective (Det.) Eugene Nagler identified a group of individuals from California and Wisconsin, to include Richard C. Roark (M/W, DOB 12/16/1996) and others that have been sending and receiving high grade marijuana and marijuana derivatives through the U.S. mail. The controlled substances are

sent from California to southeastern Wisconsin, including Milwaukee. During this investigation case agents have seized numerous suspicious packages sent from California to Wisconsin. Law enforcement officers obtained search warrants and upon searching pursuant to the warrants, found controlled substances.

14. On August 29, 2022, members of the Washington County (Wisconsin) Sheriff's Department observed Roark, driving southbound on Interstate 41, south of Lannon Road, in the Village of Germantown. Shortly thereafter, deputies observed that Roark was driving a 2022 GMC Yukon Denali (bearing Wisconsin dealer plate number APV2269). Deputies conducted a check of this license plate and determined that the license plate did not correspond to the vehicle affixed with the dealer plate. As a result, officers conducted a traffic stop. During the traffic stop, a canine alerted on the vehicle. Deputies searched the vehicle and located approximately 7,225 grams of suspected raw marijuana and three (3) Apple iPhones. Roark was driving the vehicle and Jessica Etta (W/F, DOB XX/XX/1995) was identified as the passenger. Roark was placed under arrest for possession of THC, the active ingredient in marijuana.

15. On that same date, after learning of the traffic stop involving Roark, Det. Nagler drove to Roark's residence, 13625 Hampton Road, Brookfield, Wisconsin. At approximately 3:00 p.m., Det. Nagler arrived in the area of Roark's residence. A short time later he observed Roark's mother, Shannon M. Roark (W/F, XX/XX/1980), arrive at the residence driving a blue Chevrolet Suburban (unknown plate). Shortly thereafter, Det. Nagler observed Roark's father, Richard Carl Roark (W/M, DOB XX/XX/1977) arrive driving a 2005 Cadillac Escalade SUV (bearing Wisconsin license plate number 885XWL). Both Shannon Roark and Richard Roark Sr. had been previously identified by law enforcement officers. Det. Nagler watched as Shannon Roark made several trips into the home and loaded

various boxes into the Cadillac Escalade before driving the Cadillac Escalade away from the house. At the same time, Det. Nagler observed Roark's father leave the house driving the blue Chevrolet Suburban. Det. Nagler determined the Cadillac Escalade, driven by Shannon Roark, was traveling above the speed limit as it drove eastbound on Hampton Road. Additionally, the vehicle appeared to have illegal tints. Consequently, City of Milwaukee Police Department officers initiated a traffic stop of the vehicle at 76th and Hampton in Milwaukee, Wisconsin. Upon making contact with Shannon Roark, officers immediately detected a strong odor consistent with raw marijuana emanating from inside the vehicle. The officers searched the vehicle and located the following: one 9 mm pistol with an extended magazine, but without a serial number (commonly referred to as a "ghost gun"); three (3) wristwatches (two Rolex, one Piquet); additional jewelry; approximately 1,506.5 grams of suspected raw marijuana; six mg of oxycodone; 383.9 grams of suspected THC gummies; 52 THC vape cartridges; three ounces of suspected THC concentrate; 3,428 grams of THC edibles; and, 69.5 grams of suspected THC joints.

16. During a *Mirandized* statement, Shannon Roark stated she received a phone call from a family member after the family member observed her son, Richard Roark, stopped by the police on I-41 southbound. Shannon Roark stated that she went to Roark's residence in order to retrieve her son's dog, when she observed the above-referenced items officers located in her vehicle inside her son's home. Shannon Roark stated she panicked and did not know what to do, so she took the items, loaded them into her vehicle and left the house.

17. On September 1, 2022, at 4:38 p.m. the Honorable Ryan J. Hetzel, Washington County Circuit Court Judge, authorized a search warrant of a black Apple iPhone associated with phone number 920-445-3263 seized from Jessica Etta's purse on August 29, 2022. The

investigation previously revealed, that telephone number 1-920-445-3263 is one of Richard (Ricky) Roark's "trap phones." Based upon my training and experience, I know that a "trap phone" is a telephone designated for drug trafficking business. A subpoena for records related to 920-445-3263 (IMSI: 310410222187541) revealed that it has been active since September 23, 2019, up to the present, and lists to PREPAID CUSTOMER, at 825 Shope St., Los Angeles, CA 90017.

18. A search of the aforementioned phone revealed that in the "Notes" section, there were numerous drug lists/ inventories with weights and prices for various THC products and marijuana. Specifically, law enforcement officers observed a notation stating, "Fawn - \$4,650." Additionally, 541 "chats" were recovered from this phone, many with no content, and most are drug and or drug debt related. Law enforcement officers also observed numerous Telegram chats related to international orders, shipping and methods of payment to include cryptocurrency, Zelle, cash app, cash in the mail and banks along with several chats with prospective customers from outside the U.S. I am aware that Telegram is an end-to-end encrypted application.

19. In the chats, law enforcement officers observed a chat with "Fawn" at 707-472-6505. A review of the chat revealed that Roark receives marijuana from Fawn in California which is then sent to Wisconsin. A review of subpoenaed records further reveals that Roark sends cash for the marijuana to Fawn through Zelle, a payment application. In the chats observed on Roark's "trap phone," Roark and Fawn discuss prices, quality, varieties of marijuana and the balance owed. Fawn also sent photos of large marijuana grows to Roark.

20. Case agents positively identified "Fawn" as Fawn J. Winkles (W/F, DOB XX/XX/1979), residing at 1706 North Road, Laytonville, California 95454 and using phone number 707-472-6505. Records subpoenaed for 707-472-6505 revealed that it lists to Fawn

Winkles, P.O. Box 1749 Laytonville, California. A search of a law enforcement database revealed 1706 North Road, Laytonville, California 95454 is owned by Fawn J. Winkels and associated with P.O. Box 1749, Laytonville, California 95454.

21. On February 1, 2023, U.S. Postal Inspector Tyler Fink was contacted by Milwaukee Police Department Detective Eugene Nagler in reference to an on-going drug trafficking investigation related to Fawn Winkels. Inspector Fink reviewed U.S. Postal Service (USPS) business records which revealed the following information:

22. On March 11, 2021, three USPS money orders totaling \$3,000.00 were purchased at one post office. The serial numbers of the money orders were 2655957717, 2655957718, and 2655957721, respectively. All money orders were purchased at the North Milwaukee Post Office, located at 5995 N. Teutonia Avenue, Milwaukee, Wisconsin 53209. Each money order was made payable to "Fawn Winkels," and likely cashed at post offices. Based upon his training and experience, Inspector Fink indicated that the amount of money used to purchase these money orders is inconsistent with normal USPS customer related business and indicates possible suspicious use of USPS money orders.

23. On April 18, 2022, three USPS money orders totaling \$3,000 were purchased at two different post offices in the Milwaukee, Wisconsin area. The serial numbers of the money orders were 2788461228, 2788461229, and 2816197904, respectively. Two money orders, 2788461228 and 2788461229, were purchased at the Butler Post Office, located at 1242 W. Hampton Avenue, Butler, Wisconsin 53007, totaling \$2,000.00. One money order, 2816197904, was purchased at the Wauwatosa Post Office, located at 1655 N. Mayfair Road, Milwaukee, Wisconsin 53226, totaling \$1,000.00. A review of the images of the money orders revealed that they were made payable to "Fawn Winkels," and likely cashed at a post office. Inspector Fink is

aware that the amount of money used to purchase these money orders is inconsistent with normal USPS customer related business and indicates possible suspicious use of USPS money orders.

24. Additionally, from May 2, 2022, through July 7, 2022, four USPS money orders totaling \$4,000.00 were purchased at two different post offices in the Milwaukee, Wisconsin area. The serial numbers of the money orders were 2816198079, 2788461855, 2788461856, and 2816199011, respectively. On May 2, 2022, one money order, 2816198079, was purchased at the Wauwatosa Post Office, located at 1655 N. Mayfair Road, Milwaukee, Wisconsin 53226, totaling \$1,000.00. On July 7, 2022, two money orders, 2788461855 and 2788461856, were purchased at the Butler Post Office, located at 1242 W. Hampton Avenue, Butler, Wisconsin 53007, totaling \$2,000.00. Also on July 7, 2022, one money order, 2816199011, was purchased at the Wauwatosa Post Office totaling \$1,000.00.

25. Images of the money orders show they were all made payable to "Fawn Winkels," and likely cashed at a post office. Similarly, Inspector Fink is aware that the amount of money used to purchase these money orders is inconsistent with normal USPS customer related business and indicates possible suspicious use of USPS money orders.

26. The aforementioned money orders were all purchased at post offices in the near vicinity of Ricky Roark's residence. Additionally, the purchase pattern of these money orders suggests activity used to deter law enforcement attention and an effort to avoid the reporting requirements of the Bank Secrecy Act and conceal illegal proceeds obtained from controlled substance sales.

27. In January 2023, the Mendocino County Major Crimes Task Force (MMCTF) conducted surveillance at Fawn Winkels' residence, 1706 North Road, Laytonville, California 95454. In mid-January, during the surveillance operation, MMCTF investigators observed a



white Mazda SUV (bearing California license plate number 8JRJ488) parked in front of 1706 North Road, Laytonville, California. A search of California DMV records indicated the vehicle is registered to Winkels at 1706 North Road, Laytonville, California. At this time investigators observed lights on inside the residence.

28. On January 25, 2023, MMCTF Commander (Com.) Clynton Wyant assisted California Lake County Sheriff's Office in the service of a marijuana related search warrant at 345 Branscomb Road, Laytonville California, where that suspect was also involved in transporting commercial quantities of illegal marijuana to the state of Nebraska. During the service of this search warrant, the suspect, Timothy Ray Harris (DOB 10/01/1957), was detained and later interviewed. As Com. Wyant was assisting with this particular search warrant, he overheard Sgt. Keithly of the Lake County Sheriff's Office speaking to another Lake County deputy regarding a text message conversation between Harris and a female named, "Fawn," all related to the sales of marijuana.

29. After overhearing this, it caught his attention as "Fawn" is an uncommon name and he had previously received information related to the investigation occurring in Wisconsin, involving "Fawn Winkels" of Laytonville, California.

30. Com. Wyant was then shown a text message conversation between "Fawn" and Harris. Com. Wyant asked Harris if he knew "Fawn's" last name, to which he responded, "Winkels." It should be noted, Harris was not in handcuffs, was very cooperative, and had been advised of his *Miranda* rights by the Lake County Sheriff's Office.

31. At the conclusion of their interview, Com. Wyant asked Harris if he could ask him a few questions un-related to his current predicament. Harris agreed, and told Com. Wyant the following, summarized as follows:

32. Harris confirmed the text message conversation between Harris and Winkels was regarding the sales/transportation of marijuana. Harris stated Winkels is a "marijuana broker" and coordinates large marijuana sales that usually involves numerous people to be shipped out of state. Harris stated, "Fawn is very connected and is probably the biggest marijuana broker in Laytonville." Based on the on-going investigation conducted in Wisconsin, Com. Wyant did not question Harris any further or allude to the fact Winkels was currently under investigation for commercial sales of marijuana.

33. After learning this information, Com. Wyant contacted Det. Nagler in Wisconsin.

34. On February 6, 2023, investigators from the United States National Guard Counter Drug Task Force conducted surveillance in Laytonville, California. Investigators located Winkels' vehicle (White 2019 Mazda -8JRJ488) in downtown Laytonville at a beauty salon. Shortly after locating her vehicle, Winkels was positively identified as entering the aforementioned vehicle where she was followed by the surveillance team. During the course of the surveillance, they observed Winkels entering her property/residence located at 1706 North Road, Laytonville, California.

35. On March 28, 2023, Com. Wyant, obtained a California state search warrant for 1706 North Road, Laytonville, California from California Superior Court Judge Keith A. Faulder.

36. On March 29, 2023, MMCTF executed the search warrant at 1706 North Road, Laytonville, California. Your affiant and Milwaukee Police Department Detective (Det.) Nagler were present on scene to assist with the search of the residence. Following the execution of the warrant, and prior to any questioning, your affiant and Det. Nagler provided Winkels a copy of the search warrant and stated to her that the search warrant related to her marijuana dealing

activity. Winkels responded to investigators, without questioning, “Well yeah, but everyone around her deals marijuana.” Your affiant read Winkels her *Miranda* rights. Winkles requested an attorney and no questioning then occurred.

37. During the search of the residence, investigators located the following electronic devices:

- Samsung Smarthphone (model unknown, IMEI: 352612262310911, ATF item no. 0046, **TARGET DEVICE 1**);
- Purple Apple iPhone (model unknown, serial no. unknown, ATF item no. 0052, **TARGET DEVICE 2**);
- Motorola smartphone with light blue case, ATF item no. 0053 , **TARGET DEVICE 3**);
- Black Amazon tablet (model unknown, ATF item no. 0047, **TARGET DEVICE 4**)
- Black Dell Desktop Computer (model unknown, ATF item no. 0054, **TARGET DEVICE 5**);
- Black Lenovo laptop computer (model unknown, ATF item no. 0051, **TARGET DEVICE 6**); and,
- External hard drive (make/model unknown, ATF item no. 49, **TARGET DEVICE 7**).

38. Immediately following the completion of the search warrant, Com. Wyant, turned over the electronic devices to your affiant. The items remained in your affiant’s physical custody until they were secured in the ATF Milwaukee evidence vault, 1000 N. Water Street, Suite 1400, Milwaukee, Wisconsin, on March 31, 2023, where they have remained.

39. Your Affiant believes additional information relevant to the investigation involving violations of 21 U.S.C. Sections 846 and 841 (conspiracy to distribute controlled substances and possession with intent to distribute and distribution of controlled substances) and 18 U.S.C. Sections 1956 and 1957 (conspiracy to commit money laundering and money laundering) is housed within the aforementioned **TARGET DEVICES**.

40. Your Affiant is aware that cellphones, tablets, computers and usb hard drives can be used to store information including text messages, multimedia messages, and a history of incoming and outgoing calls, contact/address book information, photographs, video and other data.

41. Similarly, your affiant is aware that many cellphones, tablets, computers and usb drives contain a list of contacts and associate names, and cellphone numbers and other identifying information. Your Affiant asks that this information be included in the search warrant, as it will assist in identifying the user/owner of the cellphone, individuals with whom the user had contact, and may provide evidence of the source of any guns involved in this investigation.

42. Your Affiant is also requesting an authorized search of cellphone devices and computers to include all removable drives, cards, memory devices or similar devices attached to or contained within said cellphone or computer. Your Affiant is aware that cellphones, tablets, and computers frequently contain SD cards or other removable memory/storage devices upon which data, including photographs, videos, and other information, may be stored.

43. Your Affiant is aware that many cellphones, tablets and computers capture or otherwise store GPS location tracking/logging files, may provide additional evidence as to the targets travels and may provide evidence as to the location where the alleged illegal actions occurred. Similarly, said information may assist law enforcement with locating and identifying other subjects with whom the target was involved in related to narcotics trafficking, including by identifying the place or places where said illegal possession of firearms and/or narcotics may have occurred.

## **TECHNICAL TERMS**

44. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored

images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer

programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

45. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

46. There is probable cause to believe that things that were once stored on the device may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before



they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

47. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes

were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the

warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

48. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

49. Manner of execution. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

## **ATTACHMENT A**

### **Property to Be Searched**

1. The property to be searched are seven (7) electronic storage devices currently held at the Bureau of Alcohol, Tobacco, Firearms and Explosives, 1000 N. Water Street, Suite 1400, Milwaukee, Wisconsin, which can be further described as:

- a. Samsung Smartphone (model unknown, IMEI: 352612262310911, ATF item no. 0046, **TARGET DEVICE 1**);
- b. Purple Apple iPhone (model unknown, serial no. unknown, ATF item no. 0052, **TARGET DEVICE 2**);
- c. Motorola smartphone with light blue case, ATF item no. 0053 , **TARGET DEVICE 3**);
- d. Black Amazon tablet (model unknown, ATF item no. 0047, **TARGET DEVICE 4**);
- e. Black Dell Desktop Computer (model unknown, ATF item no. 0054, **TARGET DEVICE 5**);
- f. Black Lenovo laptop computer (model unknown, ATF item no. 0051, **TARGET DEVICE 6**); and,
- g. External hard drive (make/model unknown, ATF item no. 49, **TARGET DEVICE 7**).

## **ATTACHMENT B**

### **Particular Things to be Seized**

1. All records on the seven electronic devices related to violations of 18 U.S.C. §§ 1956 and 1957 (conspiracy to commit money laundering and money laundering), and 21 U.S.C. §§ 846 and 841 (conspiracy to distribute, possession with intent to distribute and distribution of controlled substances) including:
  - a. lists of contacts with any identifying information;
  - b. photographs, videos, or other media storage connected to the enumerated violations;
  - c. types, amounts, and prices of drugs purchased/sold;
  - d. any information related to sources or purchasers of drugs (including names, addresses, phone numbers, or any other identifying information);
  - e. all bank records, checks, credit card bills, account information, and other financial records related to the enumerated violations.
2. Any and all financial records connected to the purchase/sale of drugs and money laundering;
3. Documentation establishing the identity of the individuals in control of the residences;
4. Any and all financial records connected to the purchase/sale of drugs and money laundering, and any correspondence regarding other drug sellers and/or purchasers;
5. Any evidence of illegal drugs or controlled substances;
6. Any evidence of proceeds of drug trafficking activities, including United States currency;

7. All bank records, checks, credit card bills, account information, and other financial records; financial records, documents, statements, or other evidence of control of bank or other financial accounts and investment funds;

8. List of drug customers and related identifying information;

9. Personal address books, telephone bills, photographs, letters, personal notes, documents and other items or lists reflecting names, addresses, telephone numbers, addresses and communications regarding illegal activities among and between members and associates involved in drug trafficking activities;

10. Any evidence of documents and deeds reflecting the purchase or lease of items obtained with the proceeds from drug trafficking activities;

11. Records of off-site locations to store proceeds and other records, including safes, vaults, or lock boxes, safe deposit box keys, records and receipts and rental agreements for storage facilities;

12. Records of mail and communications services, cellular telephones and all electronic storage areas on the devices including stored telephone numbers, recently called numbers list, text messages, digital audio and or video recordings, pictures, settings, and any other user defined settings and/or data;

13. Evidence of indicia of occupancy, residency or ownership of premises, including utility bills, telephone bills, loan payment receipts, addressed envelopes, escrow documents and keys;

14. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

15. Records evidencing the use of the Internet Protocol address, including:
  - a. records of Internet Protocol addresses used;
  - b. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.